BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

KOREAN PATENT ABSTRACT (KR)

PUBLICATION

(51) IPC Code: HO4L 12/22
(11) Publication No.: 2003-0039732 (43) Publication Date: May 22, 2003
(21) Application No.: 10-2001-0070765 (22) Application Date: November 14, 2001

(71) Applicant:
Electronics and Telecommunications Research Institute
161 Gajeong-Dong, Yuseong-Gu, Daejeon 305-350, Korea

(72) Inventor:
LEE, SEUNG MIN

NAM, TAEK YONG

LEE, SU HYUNG

JI, JEONG HOON

OH, SEUNG HEE

(54) Title of the Invention:
Attacker Traceback Method Using Log Information of Edge Router on the Internet

Abstract:

Provided is an attacker trace back method for tracing the hacking of a certain data, system or service in the global network environment of the Internet. In the prior art, since each host has a different method and format of recording log information the attack pathway of the hacker is analyzed by hand. Especially when the hacker falsifies his/her IP (Internet Protocol) address it is impossible to trace the hacker with only the log information left in the host. However in the attacker traceback method the network's location in which the hacker resides is traced even when the hacker falsifies his/her IP address and via various networks launches cyber attacks such as a Denial of Service (DOS), which stops service. Therefore companies, government organizations or even countries can be better prepared against cyber attacks from domestic and overseas hackers with a safer and more reliable Internet environment guaranteed.

(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(51) Int. Cl.
H04L 12/22

(11) 공개번호 특2003-0039731
(43) 공개일자 2003년05월22일

(21) 출원번호 10-2001-0070765
(22) 출원일자 2001년11월14일

(71) 출원인 한국전자통신연구원
대한민국
305-350
대전 유성구 가정동 161번지

(72) 발명자 이수형
대한민국
305-721
대전광역시유성구신성동153하나아파트108-505

이승민
대한민국
306-777
대전광역시대덕구송촌동461-1선비마을아파트301-502

지정훈
대한민국
138-796
서울특별시송파구잠실6동장미아파트3차1-802

오승희
대한민국
305-350
대전광역시유성구가정동236-1ETRI기숙사1동328

남택용
대한민국
305-707
대전광역시유성구신성동160-1한울아파트106-604

(74) 대리인 장성구
김원준

(77) 심사청구 있음

(54) 출원명 코드의 이동성을 적용한 세션 정보 관리를 통한 공격자 역추적 방법

요약

본 발명은 글로벌(global)하게 이루어지는 해커(hacker)의 호스트(host)에 대한 직접적인 침입공격을 탐지하였을 경우, 해커의 해당 연결을 추적하여 해커가 실제로 존재하는 호스트를 식별해내도록 하는 공격자 역 추적 방법에 관한 것이다. 종래의 기술은 특정 호스트가 속해 있는 도메인은 보호할 수 있으나 공격자를 식별할 수는 없다. 따라서, 공격자에 대한 대응을 할 수 없기 때문에, 공격자가 이전 공격에 사용했던 네트워크와 다른 네트워크에 연결된 호스트를 경유해서 동일한 호스트에 대해 제 2, 제 3의 공격을 감행할 수 있는데, 이 때에는 상기 특정 호스트가 속해 있는 도메인에서 이 공격에 대해 어떤 조치를 취할 수도 없다. 본 발명은, 코드의 이동성을 적용한 세션 정보 관리를 통해 인터넷 상의 다른 호스트를 경유한 사이버 공격에 대해서도 공격자의 위치를 추적하도록 한다. 따라서, 네트워크 보안에 있어 좀더 효과적이고 능동적인 보안을 가능하게끔 한다. 공격자의 위치를 추적하여 대처함으로써 동일한 공격자에 의해 이루어지는 제 2, 제 3의 공격을 방지할 수 있다.

대표도

도2

명세서

도면의 간단한 설명

도 1은 종래의 네트워크 보안이 이루어지는 메커니즘을 나타낸 망 구성도,

도 2는 본 발명이 적용될 네트워크 환경과 실제 적용될 경우 네트워크 보안 메커니즘의 동작 흐름을 나타낸 망 구성도,

도 3은 본 발명에 따른 추적 센서가 각 호스트를 이동하여 실행될 경우 그 실행을 보장하기 위해 갖추어야 할 실행 구조를 나타낸 개략도,

도 4는 본 발명에 따른 각 호스트에 있어서, 상대 호스트와의 연결을 나타내는 세션 정보를 모니터링하는 모니터링 센서를 특정 호스트에 탑재하는 절차를 단계별로 나타낸 순서도,

도 5는 본 발명에 따라 해커의 위치를 역 추적하는 동작을 단계별로 나타낸 순서도.

<도면의 주요부분에 대한 부호의 설명>

280 : 추적 센서 281 : 모니터링 센서

290 : 공격자 호스트 291 : 경유 호스트

292 : 도메인 관리 서버 293 : 피해 호스트

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 코드(code)의 이동성을 적용한 세션 정보 관리(session data management)를 통한 공격자 역 추적 방법에 관한 것으로, 특히, 글로벌(global)하게 이루어지는 해커(hacker)의 호스트(host)에 대한 직접적인 침입공격을 탐지하였을 경우 해커의 해당 연결을 추적하여 해커가 실제로 존재하는 호스트를 식별해내도록 하는 공격자 역 추적 방법에 관한 것이다.

일반적으로 네트워크(network) 보안은 특정 호스트에 해커의 침입을 탐지하기 위한 방법과 해커의 침입을 탐지하였을 경우 어떻게 대응할 것인가에 관한 방법으로 나누어진다.

종래의 네트워크 보안 기술은 특정 호스트가 속해있는 도메인(domain)의 보안을 어떻게 효과적으로 확보할 것인가에 초점이 맞추어져 있다. 예로, 해당 도메인의 특정 호스트에 대한 공격을 어떻게 효율적으로 탐지할 것인가에 대한 측면과 상기 특정 호스트에 대한 공격을 탐지하였을 경우 어떻게 공격자의 트래픽(traffic)을 자신의 도메인 입구에서 차단하여 상기 특정 호스트를 보호할 것인가에 대한 측면에 치중하고 있다.

이와 같은 종래의 기술은 특정 호스트가 속해 있는 도메인은 보호할 수 있으나 공격자를 식별할 수는 없다. 따라서, 공격자에 대한 대응을 할 수 없기 때문에, 공격자가 이전 공격에 사용했던 네트워크와 다른 네트워크에 연결된 호스트를 경유해서 동일한 호스트에 대해 제 2, 제 3의 공격을 강행할 수 있는데, 이 때에는 상기 특정 호스트가 속해 있는 도메인에서 이 공격에 대해 어떤 조치를 취할 수도 없다.

도 1은 종래의 네트워크 보안이 이루어지는 메커니즘을 나타낸 망 구성도로, 방화벽 시스템(150)이 침입탐지 시스템(160) 및 보안 관리 시스템(170)을 구비한 도메인(180)을 인터넷(internet)으로부터의 공격을 차단하도록 구성된다.

동 도면에 있어서, 소정의 공격자가 도메인(180)을 외부 인터넷을 통해 공격(110)하면, 도메인(180)에 설치된 침입탐지 시스템(160)은 보안 관리 시스템(170)으로 상기 공격 사실을 통보한다.

보안 관리 시스템(170)은 침입탐지 시스템(160)으로부터 공격 사실을 통보받아 도메인(180)의 입구에 설치된 방화벽 시스템(150)을 동작시켜 상기 인터넷을 통해 접속한 공격자의 트래픽을 차단시킨다(140).

상술한 도 1과 같은 경우 인터넷을 통해 들어오는 공격자로부터 도메인(180)을 방어할 수는 있지만 공격자가 경유 호스트를 변경하여 재 공격할 경우에는 공격자의 트래픽을 차단할 수 없기 때문에, 이어지는 제 2, 제 3 등의 공격을 허용할 수밖에 없다.

발명이 이루고자 하는 기술적 과제

본 발명은 상기의 문제점을 해결하기 위하여 안출한 것으로, 코드의 이동성을 적용한 세션 정보 관리를 통해 인터넷 상의 다른 호스트를 경유한 사이버 공격에 대해서도 공격자의 위치를 추적하도록 하는 코드의 이동성을 적용한 세션 정보 관리를 통한 공격자 역 추적 방법을 제공하는 데 그 목적이 있다.

이와 같은 목적을 달성하기 위한 본 발명은, 도메인 관리 서버 및 다수의 호스트를 각각 구비하는 다수의 도메인이 인터넷에 각각 접속된 통신 시스템에 있어서, 호스트의 세션을 모니터링(monitoring)하는 코드로 이루어진 모니터링 센서를 상기 각 호스트로 상기 인터넷을 통해 각각 파송해서 상기 각 호스트에 각각 탑재시켜 각 호스트의 각 세션을 각각 모니터링하는 제 1 단계; 특정 호스트가 공격당하는 경우 상기 각 호스트에 탑재된 모니터링 센서가 모니터링한 각 세션 정보를 참조하여 공격자 경로에 대응하는 다음 호스트를 찾아 공격자를 역 추적하는 제 2 단계를 포함하는 것을 특징으로 한다.

발명의 구성 및 작용

도 2는 본 발명이 적용될 네트워크 환경과 실제 적용될 경우 네트워크 보안 메커니즘의 동작 흐름을 나타낸 망 구성도로, 인터넷을 통해 각각 파송되어 다수의 호스트(290, 291, 293)에 각각 탑재된 모니터링 센서(281)가 각 호스트의 각 세션을 각각 모니터링했다가 추적 센서(280)의 공격자 접속경로정보 요구가 있을 때 추적 센서(280)에게 공격자 접속경로정보를 제공하도록 구성된다. 상기 공격자 접속경로정보는 예로, 공격자가 바로 이전에 경유했던 호스트의 위치 정보이다.

동 도면에 있어서, 먼저 모니터링 센서(281)는 고착형 프로그램 코드(program code)로, 각 호스트(290, 291, 293)에 인터넷을 통해 각각 탑재되어 각 호스트(290, 291, 293)의 각 세션을 각각 모니터링한다. 추적 센서(280)는 각 호스트(290, 291, 293)에 각각 탑재된 모니터링 센서(281)가 요구에 의해 제공하는 공격자가 바로 이전에 경유했던 호스트에 대한 접속경로정보를 수집하면서 공격자가 최초로 사용한 호스트의 위치를 역 추적한다. 상기 센서는 일반적으로 사용되고 있는 모바일 코드(mobile code)로서, 인터넷에 접속된 각 호스트에 파송해서 탑재시킬 수 있다.

예로, 침입방지 시스템은 피해 호스트(293)가 인터넷을 통해 공격당한 것이 탐지되면 이 공격당한 사실을 자신의 도메인 관리 서버로 통보(210)한다.

도메인 관리 서버는 공격당한 사실을 침입방지 시스템으로부터 통보 받을 경우 추적 센서(280)를 피해 호스트(293)로 전송(212)한다.

추적 센서(280)는 피해 호스트(293)에서 모니터링 센서(281)로부터 공격자가 바로 이전에 경유했던 호스트(291)의 위치 정보를 획득(213)하여 경유 호스트(291)로 인터넷을 통해 이동(220, 231)한다. 이 때, 도메인을 건너서 이동하는 경우 해당 도메인 관리 서버(292)로부터 추적 센서(280)의 역추적 수행을 위한 인증을 받는다(221, 230).

추적 센서(280)는 경유 호스트(291)에서 모니터링 센서(281)로부터 공격자가 바로 이전에 경유했던 호스트의 위치 정보를 획득(232)하여 해킹 호스트로 인터넷을 통해 이동해서 공격자가 로그인하여 작업 중인 공격자 호스트(290)를 추적해 낸다.

여기서, 상기 다수의 호스트(290, 291, 293)를 인터넷을 통해 주기적으로 액세스(access)하면서 모니터링 센서(281)를 이루는 코드의 무결성을 관리한다.

도 3은 본 발명에 따른 추적 센서(280)가 각 호스트(290, 291, 293)를 이동하여 실행될 경우 그 실행을 보장하기 위해 갖추어야 할 실행 구조를 나타낸 개략도로, 호스트를 구동하기 위한 기본적인 커널(360)과 운영체제(380)가 존재하고 일반적인 응용 프로그램(370)은 운용체제 상에서 실행된다. 상기 운영체제(380)는 호스트를 운영하기 위한 윈도우즈 NT 등의 프로그램으로, 호스트 내의 하드디스크(Hard Disk Drive : HDD) 등에 저장되어 있다가 호스트를 최초로 부팅(booting)할 때 실행되고 일부는 호스트 내의 주 메모리(main memory) 등에 탑재된다.

독립적인 실행 환경을 역 추적용 센서(310)에게 제공하기 위한 센서실행엔진(330)이 각 호스트(290, 291, 293)의 각 운영체제(380) 위에 각기 탑재된다. 운영체제 인터페이스(operating system interface)(350)는 운영체제(380)와 센서실행엔진(330), 응용 프로그램(370)간을 인터페이스 시켜준다. 센서실행엔진(330)은 센서(310) 자체의 기능 수행을 위해 필요한 센서실행 라이브러리(340)를 포함한다. 센서실행 라이브러리(340)의 기능을 보면, 센서(310) 이동상의 센서(310) 자체의 보안을 위한 센서(310) 보안 기능, 센서(310)의 이동 생성 및 소멸을 관리하기 위한 센서(310) 관리 기능, 센서(310)간의 통신을 위한 센서(310) 통신 기능 등이 있다. 센서(310)는 실행되기 위해 필요로 하는 센서실행엔진(330)의 기능을 센서 응용프로그램 인터페이스(Application Program Interface : API)(320)를 통해 제공받아 센서실행엔진(330) 상에서 실행된다.

도 4는 본 발명에 따른 각 호스트에 있어서, 상대 호스트와의 연결을 나타내는 세션 정보를 모니터링하는 모니터링 센서를 특정 호스트에 탑재하는 절차를 단계별로 나타낸 순서도이다.

먼저, 모니터링 센서를 탑재할 호스트의 타입을 판단한다(단계 420).

단계 420에서 호스트의 타입을 판단한 결과, 모니터링을 위한 새로운 기법이 개발되었을 경우 상기 모니터링 센서를 탑재할 호스트의 도메인 관리 서버는 상기 호스트의 유형에 적합한 모니터링 센서를 생성한다(단계 430).

상기 도메인 관리 서버에 생성한 모니터링 센서를 저장하고 상기 단계 420을 수행한다(440).

단계 420에서 호스트의 타입을 판단한 결과, 모니터링 센서를 탑재할 호스트가 새로운 호스트일 경우 그 호스트에게 자신의 운영체제 및 응용 유형을 질의한다(단계 460).

상기 질의 응답에 따라 적합한 모니터링 센서를 선택한다(단계 470).

상기 선택된 적합한 모니터링 센서를 상기 질의 대상 호스트로 이동시킨다(단계 480).

상기 질의 대상 호스트의 센서 실행 엔진에 상기 선택된 적합한 모니터링 센서를 탑재시킨다(단계 490).

도 5는 본 발명에 따라 해커의 위치를 역 추적하는 동작을 단계별로 나타낸 순서도이다.

먼저, 보안관리 시스템은 자신이 속한 도메인의 호스트가 공격받음에 따른 침입을 침입탐지 시스템이 탐지했는지 여부를 판단한다(단계 510).

보안관리 시스템은 침입탐지 시스템이 침입을 탐지했을 경우 역 추적 센서를 생성한다(단계 520).

보안관리 시스템은 생성한 역 추적 센서를 공격받고 있는 침입대상 호스트로 이동시킨다(단계 530).

침입대상 호스트로 이동된 역 추적 센서는 침입대상 호스트에서 세션을 모니터링 중인 모니터링 센서에게 공격자의 이전 경로 정보를 질의한다(540).

역 추적 센서는 모니터링 센서에게 공격자의 이전 경로 정보를 받아 이에 대응하는 다음 호스트가 자신의 도메인과 다른 도메인에 존재하는지 여부를 판단한다(단계 550).

다음 호스트가 다른 도메인에 존재하는 경우 다른 도메인의 관리 서버에게 역 추적 센서에 대한 인증을 의뢰한다(560).

역 추적 센서는 다른 도메인의 다른 호스트로 이동한다(단계 570).

역 추적 센서는 다른 호스트에 탑재된 모니터링 센서에게 역 추적 경로 상의 다음 호스트 경로를 질의하고 상기 단계 550을 수행한다(580).

역 추적 센서는 다음 호스트가 같은 도메인에 존재하는 경우 이를 피해 호스트가 있는 도메인의 보안 관리 서버로 통보한다(590).

이와 같은 본 발명은 코드의 기능이 업그레이드되었을 경우 이를 각 도메인의 관리 서버를 통하여 해당 도메인 내의 각 호스트로 이동시킨다.

발명의 효과

상술한 본 발명은, 코드의 이동성을 적용한 세션 정보 관리를 통해 인터넷 상의 다른 호스트를 경유한 사이버 공격에 대해서도 공격자의 위치를 추적하도록

한다. 따라서, 네트워크 보안에 있어 좀더 효과적이고 능동적인 보안을 가능하게끔 한다. 공격자의 위치를 추적하여 대처함으로써 동일한 공격자에 의해 이루어지는 제 2, 제 3의 공격을 방지할 수 있다. 공격자의 위치를 식별함으로써 공격자에 대한 글로벌한 수준에서의 대응이 가능함으로써 사이버 공격에 대한 대처 능력을 급격히 향상시킬 수 있다. 보안 관련 기능을 수행하는 코드에 이동성을 부여함으로써 각 호스트별 환경에 적합한 부가적인 기능을 수행하여 글로벌한 수준에서의 효율적인 보안 기능을 수행할 수 있는 방법을 제공한다. 이동되는 코드의 실행 엔진을 각 호스트에 탑재함으로써 기능의 향상이나 새로운 기능이 개발되었을 경우 이를 신속하고 효율적으로 전체 보안 구조에 적용할 수 있다.

(57) 청구의 범위

청구항 1.
도메인 관리 서버 및 다수의 호스트를 각각 구비하는 다수의 도메인이 인터넷에 각각 접속된 통신 시스템에 있어서,

호스트의 세션을 모니터링하는 코드로 이루어진 모니터링 센서를 상기 각 호스트로 상기 인터넷을 통해 각각 파송해서 상기 각 호스트에 각각 탑재시켜 각 호스트의 각 세션을 각각 모니터링하는 제 1 단계;

특정 호스트가 공격당하는 경우 상기 각 호스트에 탑재된 모니터링 센서가 모니터링한 각 세션 정보를 참조하여 공격자 경로에 대응하는 다음 호스트를 찾아 공격자를 역 추적하는 제 2 단계를 포함하는 코드의 이동성을 적용한 세션 정보 관리를 통한 공격자 역 추적 방법.

청구항 2.
제 1 항에 있어서,

상기 역 추적을 수행하기 위한 실행 구조는, 상기 역 추적을 수행하기 위한 역 추적용 센서;

상기 각 호스트의 각 운영체제 위에 각기 탑재되어, 상기 센서 자체의 기능 수행을 위해 필요한 센서실행 라이브러리를 구비하고 독립적인 실행 환경을 상기 센서에게 제공하기 위한 센서실행엔진;

상기 운영체제와 상기 센서실행엔진, 응용 프로그램간을 인터페이스 시켜주는 운영체제 인터페이스로 이루어지는 것을 특징으로 하는 코드의 이동성을 적용한 세션 정보 관리를 통한 공격자 역 추적 방법.

청구항 3.
제 1 항에 있어서,

상기 모니터링 센서를 특정 대상 호스트에 탑재하는 과정은, 상기 특정 대상 호스트의 타입을 판단하는 제 31 단계;

호스트의 타입을 판단한 결과, 모니터링을 위한 새로운 기법이 개발되었을 경우 상기 특정 대상 호스트의 도메인 관리 서버는 상기 특정 대상 호스트의 유형에 적합한 모니터링 센서를 생성하는 제 32 단계;

상기 도메인 관리 서버에 상기 생성한 모니터링 센서를 저장하고 상기 제 31 단계를 수행하는 제 33 단계;

호스트의 타입을 판단한 결과, 상기 특정 대상 호스트가 새로운 호스트일 경우 상기 특정 대상 호스트에게 자신의 운영체제 및 응용 유형을 질의하는 제 34 단계;

상기 질의 응답에 따라 적합한 모니터링 센서를 선택하는 제 35 단계;

상기 선택된 적합한 모니터링 센서를 상기 특정 대상 호스트에 탑재시키는 제 36 단계를 포함하는 것을 특징으로 하는 코드의 이동성을 적용한 세션 정보 관리를 통한 공격자 역 추적 방법.

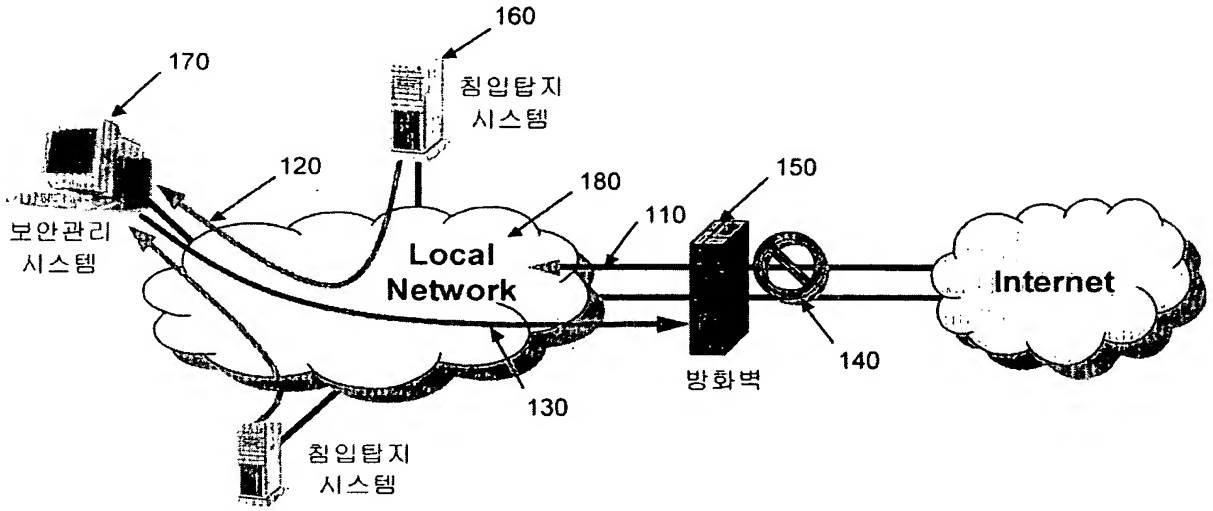
청구항 4.
제 1 항 내지 제 3 항 중 적어도 어느 한 항에 있어서, 상기 다수의 호스트를 상기 인터넷을 통해 주기적으로 액세스하면서 상기 코드의 무결성을 관리하는 단계를 더 포함하는 것을 특징으로 하는 코드의 이동성을 적용한 세션 정보 관리를 통한 공격자 역 추적 방법.

청구항 5.
제 1 항 내지 제 3 항 중 적어도 어느 한 항에 있어서, 상기 코드의 기능이 업그레이드되었을 경우 이를 각 도메인 관리 서버를 통하여 해당 도메인 내의 각 호스트로 이동시켜 상기 각 호스트에 탑재된 코드의 기능을 업그레이드시키는 단계를 더 포함하는 것을 특징으로 하는 코드의 이동성을 적용한 세션 정보 관리를 통한 공격자 역 추적 방법.

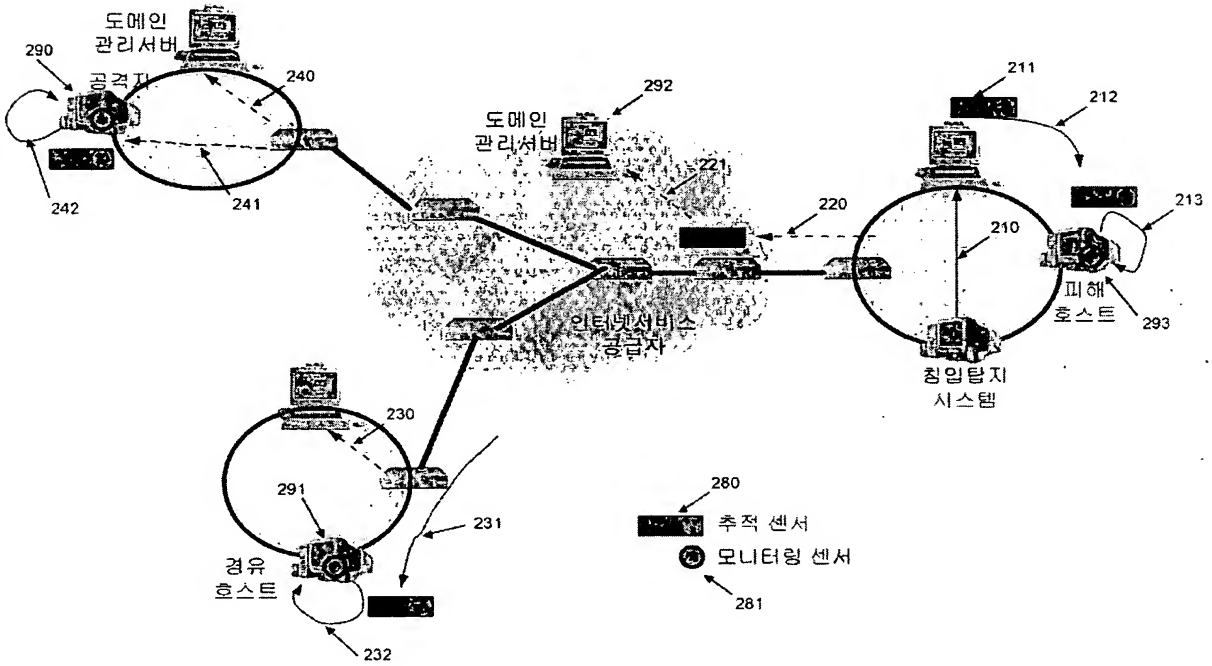
청구항 6.
제 1 항 내지 제 3 항 중 적어도 어느 한 항에 있어서, 상기 공격자 경로에 대응하는 다음 호스트가 자신과는 다른 도메인에 존재하는 경우 공격자 역 추적에 대한 인증 절차를 수행하는 단계를 더 포함하는 것을 특징으로 하는 코드의 이동성을 적용한 세션 정보 관리를 통한 공격자 역 추적 방법.

도면

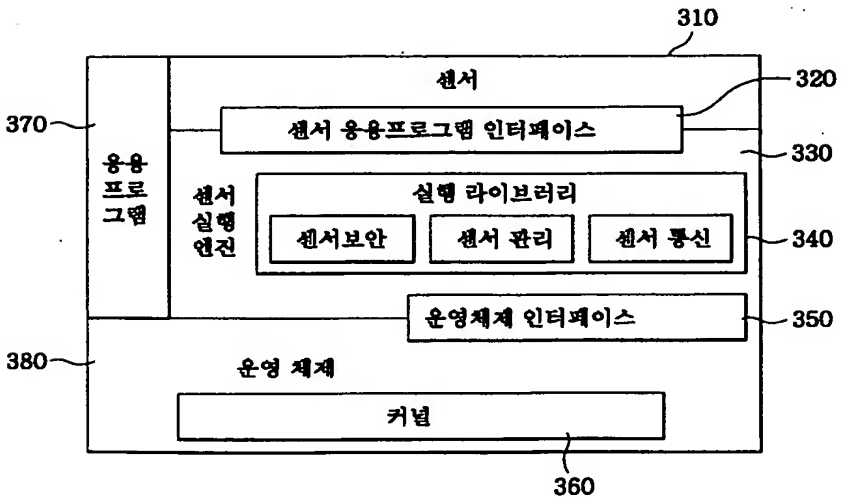
도면 1


160
침입탐지
시스템
170
120
180
150
110
보안관리
시스템
Local
Network
Internet
140
방화벽
130
침입탐지
시스템

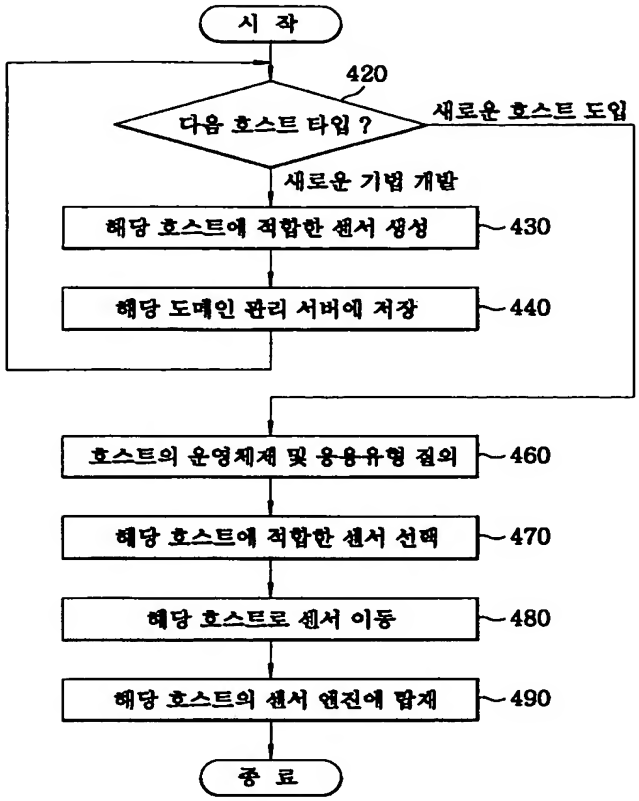
도면 2


도메인
관리서버
290
공격자
240
292
도메인
관리서버
211
212
221
220
213
210
242
241
피해
호스트
293
인터넷서비스
공급자
침입탐지
시스템
230
280
291
추적 센서
231
모니터링 센서
경유
호스트
281
232

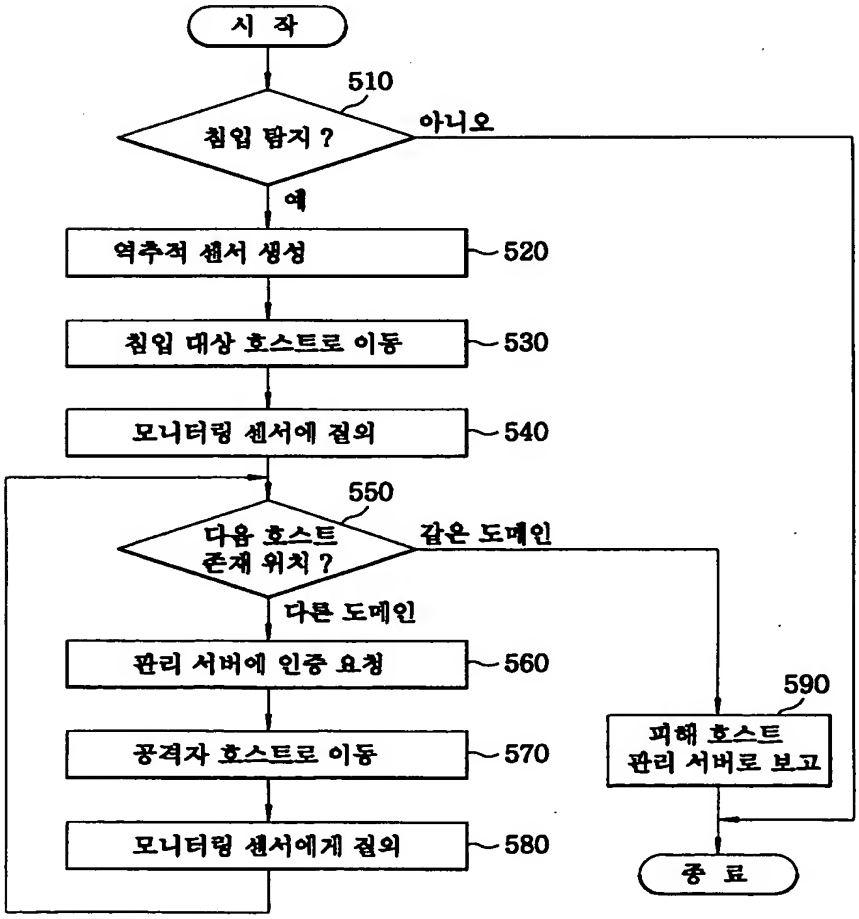
도면 3


310
센서
320
370
센서 응용프로그램 인터페이스
330
응용
프로
그램
센서
실행
엔진
실행 라이브러리
센서보안
센서 관리
센서 통신
340
운영체제 인터페이스
350
380
운영 체제
커널
360

도면 4


시 작
420
다음 호스트 타입 ?
새로운 호스트 도입
새로운 기법 개발
해당 호스트에 적합한 센서 생성
430
해당 도메인 관리 서버에 저장
440
호스트의 운영체제 및 응용유형 질의
460
해당 호스트에 적합한 센서 선택
470
해당 호스트로 센서 이동
480
해당 호스트의 센서 엔진에 탑재
490
종 료

도면 5


시 작
510
침입 탐지 ?
아니오
예
역추적 센서 생성
520
침입 대상 호스트로 이동
530
모니터링 센서에 질의
540
550
다음 호스트 존재 위치 ?
같은 도메인
다른 도메인
관리 서버에 인증 요청
560
590
피해 호스트 관리 서버로 보고
공격자 호스트로 이동
570
모니터링 센서에게 질의
580
종 료